



MUTUAL AUTHENTICATION METHOD, RECORDING DEVICE, REPRODUCING DEVICE, AND RECORDING MEDIUM

Patent number: JP2000357213
Publication date: 2000-12-26
Inventor: KAMIBAYASHI TATSU; YAMADA HISASHI; IWASAKI HIROSHI; TAMURA MASABUMI; ISHIBASHI YASUHIRO; KATO HIROSHI; TATEBAYASHI MAKOTO; HARADA TOSHIHARU
Applicant: TOSHIBA CORP.; MATSUSHITA ELECTRIC IND CO LTD
Classification:
 - international: G06K17/00; G06F3/06; G06F15/00
 - european:
Application number: JP19990170187 19990616
Priority number(s):

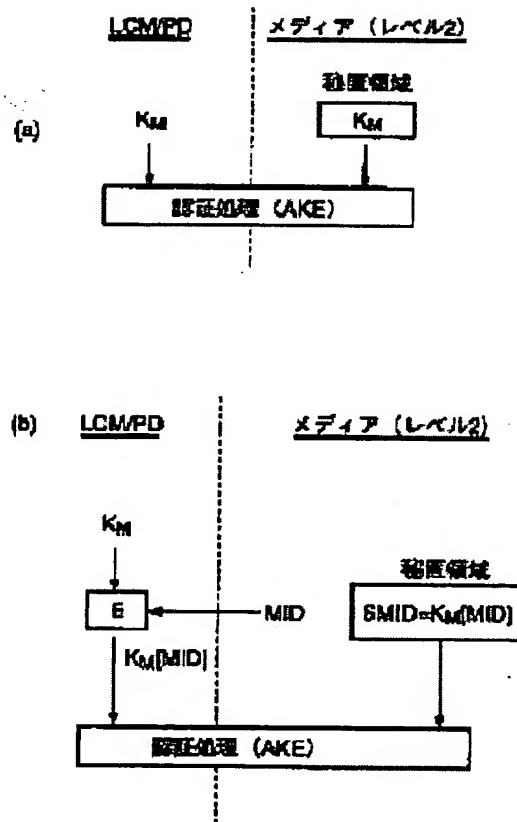
Also published as:

 EP1061514 (A2)
 EP1061514 (A3)

Abstract of JP2000357213

PROBLEM TO BE SOLVED: To use a low-cost recording medium and to realize safe mutual authentication of high security.

SOLUTION: With respect to a mutual authentication method between a recording device which records copy contents in a recording medium having an arithmetic processing function and this recording medium, first information dependent upon at least the recording medium and second information which should be shared with the recording device at the time of mutual authentication with the recording device and is dependent upon the recording medium are stored in the recording medium. The recording device generates authentication information used for mutual authentication with the recording medium based on the first information obtained from the recording medium, and this generated authentication information and the second information are used to perform mutual authentication between the recording device and the recording medium.



Data supplied from the esp@cenet database - Worldwide

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-357213

(P2000-357213A)

(43) 公開日 平成12年12月26日 (2000. 12. 26)

(51) Int.Cl. ⁷	識別記号	F I	テマコード ⁸ (参考)
G 0 6 K 17/00		G 0 6 K 17/00	T 5 B 0 5 8
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 H 5 B 0 6 5
15/00	3 3 0	15/00	3 3 0 B 5 B 0 8 5

審査請求 未請求 請求項の枚数 8 O L (全 18 頁)

(21) 出願番号 特願平11-170187

(22) 出願日 平成11年6月16日 (1999. 6. 16)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外5名)

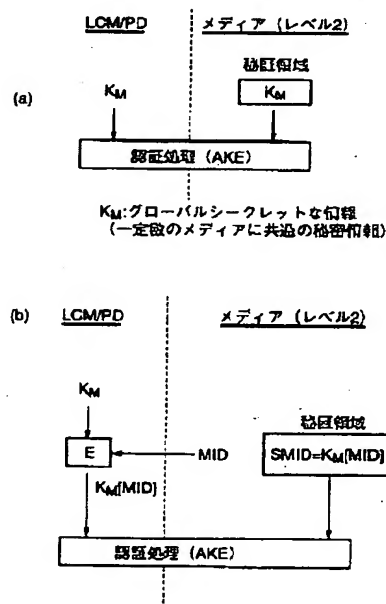
最終頁に続く

(54) 【発明の名称】 相互認証方法および記録装置および再生装置および記録媒体

(57) 【要約】

【課題】低コストな記録媒体を用いて、セキュリティ性の高い安全な相互認証が実現できる。

【解決手段】演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置と該記録媒体との間の相互認証方法において、前記記録媒体は、少なくとも該記録媒体に依存する第1の情報と、前記記録装置と相互認証を行う際に該記録装置と共有すべき該記録媒体に依存する第2の情報とを記憶し、前記記録装置は、前記記録媒体から得られた前記第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第2の情報とを用いて前記記録装置と前記記録媒体との間で相互認証を行うことを特徴とする。



【特許請求の範囲】

【請求項1】 演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置と該記録媒体との間の相互認証方法において、

前記記録媒体は、少なくとも該記録媒体に依存する第1の情報と、前記記録装置と相互認証を行う際に該記録装置と共有すべき該記録媒体に依存する第2の情報とを記憶し、

前記記録装置は、前記記録媒体から得られた前記第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第2の情報とを用いて前記記録装置と前記記録媒体との間で相互認証を行うことを特徴とする相互認証方法。

【請求項2】 演算処理機能を有する記録媒体に記録された複製コンテンツを再生する再生装置と該記録媒体との間の相互認証方法において、

前記記録媒体は、少なくとも該記録媒体に依存する第1の情報と、前記再生装置と相互認証を行う際に該再生装置と共有すべき該記録媒体に依存する第2の情報とを記憶し、

前記再生装置は、前記記録媒体から得られた前記第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第2の情報とを用いて前記再生装置と前記記録媒体との間で相互認証を行うことを特徴とする相互認証方法。

【請求項3】 前記記録媒体から得られた暗号鍵で前記第1の情報を暗号化して前記認証情報を生成することを特徴とする請求項1または2記載の相互認証方法。

【請求項4】 記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置において、

前記記録媒体から得られた該記録媒体に依存する第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、
を具備したことを特徴とする記録装置。

【請求項5】 前記記録媒体から得られた暗号鍵で前記第1の情報を暗号化して前記認証情報を生成することを特徴とする請求項4記載の記録装置。

【請求項6】 記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に記録された複製コンテンツを再生する再生装置において、

前記記録媒体から得られた該記録媒体に依存する第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、

この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、

を具備したことを特徴とする再生装置。

【請求項7】 前記記録媒体から得られた暗号鍵で前記第1の情報を暗号化して前記認証情報を生成することを特徴とする請求項6記載の再生装置。

【請求項8】 演算処理機能を有する記録媒体であって、

自己に固有の第1の情報と、記録媒体に複製コンテンツを記録する記録装置および複製コンテンツを再生する再生装置との間で相互認証を行う際に該記録装置および該再生装置と共有すべき該記録媒体に依存する第2の情報とを予め記憶した記憶手段と、

前記記録装置および再生装置にて前記第1の情報に基づき生成された認証情報と、前記第2の情報とを用いて自己と前記記録装置および自己と前記再生装置との間で相互認証を行う相互認証手段と、
を具備したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理方法を用いた記録装置、再生装置、記録媒体の間の相互認証方法およびそれを用いた記録装置、再生装置、記録媒体に関する。

【0002】

【従来の技術】従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【0003】さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと対照的に、移動は、異なった場所（記録媒体（メディア））にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【0004】

【発明が解決しようとする課題】近年、ネットワーク等を通じたオリジナルに忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的の（移動による）配布は、著作権管理を行うことができない。

【0005】このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【0006】そこで、本発明は、低コストの記録媒体を用いて、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間の高い情報セキュリティ性を実現することが可能な相互認証方法お

よび、それを用いたコンテンツの記録装置、再生装置、記録媒体を提供することを目的とする。本発明は、特に、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理に有効である。

【0007】

【課題を解決するための手段】(1) 本発明の相互認証方法は、演算処理機能を有する記録媒体に複製コンテンツを記録する記録装置(演算処理機能を有する記録媒体に記録された複製コンテンツを再生する再生装置)と該記録媒体との間の相互認証方法において、前記記録媒体は、少なくとも該記録媒体に依存する第1の情報と、前記記録装置(再生装置)と相互認証を行う際に該記録装置(再生装置)と共有すべき該記録媒体に依存する第2の情報とを記憶し、前記記録装置(再生装置)は、前記記録媒体から得られた前記第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる認証情報を生成し、この生成された認証情報と前記第2の情報とを用いて前記記録装置(再生装置)と前記記録媒体との間で相互認証を行うことを特徴とする。

【0008】本発明によれば、記録媒体にグローバルシークレットな情報(全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報)を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【0009】(2) 本発明の記録装置は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置において、前記記録媒体から得られた該記録媒体に依存する第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、を具備する。

【0010】本発明によれば、記録媒体にグローバルシークレットな情報(全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報)を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【0011】(3) 本発明の再生装置は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に記録された複製コンテンツを再生する再生装置において、前記記録媒体から得られた該記録媒体に依存する第1の情報に基づき該記録媒体との間の相互認証を行う際に用いる該記録媒体と共有すべき認証情報を生成する生成手段と、この生成手段で生成された認証情報を用いて前記記録媒体との間で相互認証を行う相互認証手段と、を具備する。

【0012】本発明によれば、記録媒体にグローバルシークレットな情報(全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報)を記録する必要がないので、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【0013】(4) 本発明の記録媒体は、演算処理機能を有する記録媒体であって、自己に固有の第1の情報と、記録媒体に複製コンテンツを記録する記録装置および複製コンテンツを再生する再生装置との間で相互認証を行う際に該記録装置および該再生装置と共有すべき該記録媒体に依存する第2の情報とを予め記憶した記憶手段と、前記記録装置および再生装置にて前記第1の情報に基づき生成された認証情報と、前記第2の情報とを用いて自己と前記記録装置および自己と前記再生装置との間で相互認証を行う相互認証手段と、を具備する。

【0014】本発明によれば、記録媒体にグローバルシークレットな情報(全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報)を記録する必要がないので、記録媒体と該記録媒体に複製コンテンツを記録する記録装置との間、記録媒体と該記録媒体に記録された複製コンテンツを再生する再生装置との間で高い情報セキュリティ性を有する相互認証が低コストの記録媒体を用いて実現できる。

【0015】

【発明の実施の形態】以下、本発明の一実施形態について図面を参照して説明する。

【0016】図1は、本実施形態にかかる記録媒体(メディア)に記憶できる複製コンテンツの数を規制し、メディアへの複製コンテンツの記録、メディアに記録された複製コンテンツの再生等を行う音楽コンテンツ利用管理システム(以下、簡単にLCMと呼ぶことがある)1の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らず、映画や、ゲームソフト等であってもよい。また、メディアとしてメモ리카ード(MC)を用いているが、この場合に限るものではなく、フロッピーディスク、DVD等の各種記録媒体であってもよい。

【0017】EMD(Electronic Music Distributor)は、音楽配信サーバまたは音楽配信放送局である。

【0018】コンテンツ利用管理システム1は、例えば、パソコン(PC)であり、複数のEMD(ここでは、EMD#1~#3)に対応した受信部#1~#3を具備しており、EMDが配信する暗号化コンテンツまたはそのライセンス(利用条件と暗号化コンテンツの復号鍵Kc)などを受信する。受信部#1~#3は、再生機能や課金機能を有していても良い。配信された音楽コンテンツを試聴する為に再生機能が用いられる。又、課金機能を利用して、気に入ったコンテンツを購入する事が

可能である。

【0019】LCM1は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：SMSで、以下、簡単にSMSと呼ぶことがある）2を具備し、利用者が購入したコンテンツはEMDインタフェース（I/F）部3を経由してSMS2に蓄積される。音楽コンテンツは、必要に応じてEMD I/F部3で復号され、形式変換や再暗号化が施される。SMS2が暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵をライセンス格納部9に格納する。SMS2が再生機能を有していても良い。当該再生機能により、SMS2が管理する音楽コンテンツをPC上で再生する事ができる。

【0020】SMS2は、メディア（以下、簡単にMC（memory card）と呼ぶことがある）13に対してコンテンツデータを出力する機能を有している。MC13を記録再生装置（以下、簡単にPD（Portable Device）と呼ぶことがある）12にセットし、MC13に記録されたコンテンツを再生することができる。

【0021】SMS2からMC13へのコンテンツの記録はメディア（MC）インタフェース（I/F）部6を通じて直接行われるか、又はPD12を経由して行うことができる。

【0022】デバイスID格納部4は、例えば、ROMで構成され、当該LCMの識別情報（デバイスID）が格納されている。

【0023】MC13は、そのメディア固有かつ書き換え不能の識別情報（MID）を有しており、MC13に格納されるコンテンツは、MC13に依存する暗号化鍵で暗号化されていてもよい。

【0024】まず、チェックイン／チェックアウトについて、図1のLCM1に則して説明する。

【0025】チェックアウトとは、LMS1が「親」としてのコンテンツを格納しており、MC13に、その複製を「子」コンテンツとしてコピーすることをいう。

「子」コンテンツはPD12で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、MC13をLCM1に接続し、LCM1が「子」コンテンツを消去（又は利用不能）する事で、LCM1内の「親」コンテンツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0026】このチェックイン／チェックアウトを単純に、従来からのLCM1で実現しようとすると、実際、次の様な「攻撃」が存在する。すなわち、MC13に格納された「子」を別の記憶メディアに（MIDを除いて）退避しておき、MC13の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該

MC13に書き戻す。既にチェックインは済んでいるので、LCM1上の「親」は別のMC13に「子」をコピーして良い。この方法で、任意の個数だけ利用可能な「子」を作る事が可能である。

【0027】上述の「攻撃」には、MC13とLCM1とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、MC13は正当なLCM1以外からのデータ転送を受け付けず、LCM1が正当なMC13以外からのデータ転送を受け付けないと仮定する。この場合、MC13内の「子」を別の記録メディアに退避する事はできない。又、LCM1に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。

【0028】ところが、実は、LCM1とMC13との認証を前提としても、チェックイン／チェックアウトは実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、LCM1上の「親」が「子」を作っていない状態で、LCM1のデータ（特に、ライセンス格納部9の情報）を別の記憶メディアにバックアップする。MC13に「子」をコピーした後、バックアップしたLCM1のデータを復帰する。LCM1の「親」は「子」を作る前の状態に戻るから、別のMC13に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。

【0029】そこで、このような攻撃にも対処できるチェックイン／チェックアウトを実現するために、MC13内の記憶領域に、公開された手順では読み書きできない領域（秘匿領域）を設け、そこに相互認証に必要な情報やコンテンツ復号に必要な情報や、アクセス不可能であるデバイス（LCM1、PD12）の識別情報（デバイスID）のリスト（リボケーションリスト（RVCリスト））等を記録する（図2参照）。また、LCM1の記憶領域（例えば、LCM1がPCで構成されている場合には、ハードディスク（HDD））上に非公開の手順でしかアクセスできない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図2参照）。さらに、PD12の記憶領域上にも非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図2参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【0030】図1に示すように、LCM1では、秘匿領域には、宿帳格納部8が設けられ、SMS2にてこの宿帳格納部8にアクセスするための秘匿された特定の手续が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ7を具備している。

【0031】図4（c）に示すように、MC13は、その識別情報MIDを格納するための外部からは書換不可能で、コピーも不可能なような構成になっている識別情

報格納部（ROM）13bと、秘匿領域13cと、公開領域（読み書き可能なRAM）13aと、秘匿領域13cにアクセスされる度に認証部13dにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域13cにアクセス可能なようにゲートを開くスイッチ（SW）13eを具備する。

【0032】なお、本実施形態で利用可能なMC13は、3種類あり、図4（c）に示すような、識別情報MIDと秘匿領域とを両方兼ね備えているMC13の種別を「レベル2」と呼ぶ。秘匿領域は持たないが識別情報MIDは持つ図4（b）に示すようなMC13の種別を「レベル1」と呼ぶ。秘匿領域も識別情報も持たない図4（a）に示すような公開領域だけのMC13の種別を「レベル0」と呼ぶことにする。これら種別は、例えば、識別情報MIDの有無でレベル0とそれ以外の種別とが判別でき、さらに、識別情報MIDの構成からレベル1とレベル2とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル2であるとする。

【0033】以下、特に断らない限り、レベル2のMC13の場合を例にとり説明する。

【0034】このMC13は、LCM1に接続されたPD12にセットして用いる場合とLCM1に直接セットして用いる場合とがある。

【0035】図3は、PD12の構成例を示したもので、MC13は、メディアインタフェース（I/F部）12fにセットされる。LCM1がPD12を介してMC13に読み書きする場合は、PD12内の秘匿領域アクセス部を経由してMC13の秘匿領域にアクセスする。メディアI/F部12fには、MC13の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。PD12内の秘匿領域は、フラッシュメモリ12dに設けられていても良い。ROM12cには、MC13、LCM1との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証手続を記述したプログラムも書き込まれていて、このプログラムに従って、CPU12aの制御の下、MC13との間の各種認証、種別判別等の処理を実行するようになっている。

【0036】ROM12cには、PD12の識別情報（デバイスID）が格納されていてもよい。また、例えば、フラッシュメモリ12dに設けられた秘匿領域に秘匿デバイスID（SPDID）が予め格納されている。

【0037】図5は、LCM1のメディアI/F部6の構成を示したもので、MC13との間で相互認証を行うための認証部6cと、MC13の種別を判別するメディア判別部6bと、これら全体を制御するための制御部6aとから構成されている。認証部6cは、MC13の秘匿領域にアクセスするための秘匿領域アクセス部でもある。

【0038】次に、LCM1の秘匿領域に格納される宿帳について説明する。

【0039】SMS2にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツID（TID）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部8に図7（a）に示すような形態で記録されている。

【0040】図7（a）において、例えば、コンテンツID「TID1」なる子の残数は「2」で、そのチェックアウトリストはL1である。

【0041】チェックアウトリストは、複製コンテンツ（子）を記録したMC13の識別情報のリストであって、例えば、図7（a）において、チェックアウトリストL1には「m1」と「m2」という識別情報を持つ2つのMC13にコンテンツID「TID1」なるコンテンツの子がチェックアウトされていることがわかる。

【0042】以下、次に示す項目の順に説明する。

【0043】（1）本発明の要旨である相互認証方法の概略

（2）レベル2のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

（3）レベル0のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

（1）本発明の要旨である相互認証方法の概略

前述したように、チェックイン/チェックアウトを安全に行うために、LCM1、PD12とMC13との間で

（例えば、互いに同じアルゴリズムをもっているかの確認のための）相互認証を行う必要がある。一般に、相互認証処理には、相互認証を行う一方と他方とで共有する秘密の情報を持つ必要がある。従って、このような秘密情報を例えばMC13とLCM1およびPD12が持つことになる。情報セキュリティの観点から考えると、この秘密情報は、認証を行う度に毎回異なるものが生成されるといった動的なものであった方がよい。しかし、MC13というメディア自体にそのような秘密情報を生成するための高度な機能を追加すると、メディアが高価になってしまう。メディアを広く一般大衆に普及させるためには、できるだけ安価である方が望ましい。従って、メディア（MC13）のコスト低減化を考えれば、秘密情報をMC13に予め記憶させておく方がよい。

【0044】しかし、全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報（以下、このような情報をグローバルシークレットな情報と呼ぶ）を各メディアに予め記憶させた場合、ある1つのメディアからその秘密情報が何らかの方法により読まれてしまったとき、同じ秘密情報を記憶する他のメディアも不正に利用されてしまうという問題点があった。メディアにグローバルシークレットな情報を持たせることは極めて危険

である(図8(a)参照)。

【0045】ある1つのメディアに記憶されている秘密情報が不当に読まれてしまっても、不正に使用できるのは、その秘密情報が読まれたメディアだけであれば問題がないわけであるから、秘密情報は、個々のメディアに固有のものであればよい。

【0046】そこで、本発明は、個々のメディアにメディア毎にそれぞれ異なる相互認証のための秘密情報を記憶させておき、この情報を用いてLCM1あるいはPD12とMC13とが相互認証を行うことにより、低コストなメディアを用いた、よりセキュリティ性の高い安全な相互認証方法を提供することを目的とする。すなわち、本実施形態で説明する相互認証方法は、図8(b)に示すように、個々のメディア(レベル2のメディア)に相互認証(AKE)のために必要な各メディア毎にそれぞれ異なる秘密情報(ここでは、秘匿メディアID(SMID))で、これは、メディアIDを何らかの方法で取得した鍵情報KMで予め暗号化されたものを(秘匿領域に)予め記憶させておき、LCM1、PD12には、そのメディアの識別情報(MID)を転送する。LCM1あるいはPD12側では、MIDと、先に何らかの方法で取得した情報(KM)とを用いて相互認証のための情報(メディアのもつSMIDと同じもの)を所定のアルゴリズムを用いて生成して認証処理(AKE)を行う。

【0047】このように、MC13にはそれぞれに固有の秘密情報(SMID)を持たせておくだけで、LCM1、PD12がメディアから転送されてきた各メディア毎に固有の情報(MID)を基に秘密情報(SMID)を生成することにより、メディアに負荷をかけずに安全な相互認証が行える。

【0048】なお、以下の説明において、本発明の要旨にかかる相互認証処理をAKEと呼ぶことにする。

【0049】MC13がLCM1のメディアI/F部6、あるいは、PD12にセットされると、まず、メディアI/F部6とMC13との間、あるいは、PD12とMC13との間で相互認証が行われてもよい(図9のステップS1)、そして、双方にて正当な(例えば、同じ規格のハードウェア構成である)相手であると判断されたとき(ステップS2)、メディアI/F部6あるいはPD12はMC13から読み取った識別情報MIDを基に、MC13の種別を判別する(ステップS3)。そして、メディアI/F部6あるいはPD12は、その種別に応じたチェックイン/チェックアウト/再生処理を実行する(ステップS6)。

【0050】なお、図9のステップS1における相互認証は、必ずしも図8(b)に示したような本発明の要旨にかかる相互認証である必要はない。

【0051】また、MC13にはレベル0からレベル2までの3種類があると説明したが、ここでは、レベル0

とレベル2の2種類のMC13を対象として、図9以降の複製コンテンツのチェックイン/チェックアウト/再生処理動作について説明する。

【0052】さらに、以下の説明では、省略しているが、LCM1とMC13との間、LCM1とPD12との間、PD12とMC13との間で、それぞれの秘匿領域にアクセスする際には、一方と他方との間で相互認証を行い、双方の正当性が確認されたらそれぞれの秘匿領域へのゲートを開き、秘匿領域へのアクセスが終了したら秘匿領域へのアクセスを可能にしていたゲートを閉じる仕組みになっているものとする。例えば、LCM1とMC13との間において、SMS2は、MC13の秘匿領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲートが開かれると、秘匿領域13c内に鍵情報書込み、それが終了すると秘匿領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。

【0053】(2) レベル2のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生
図4(c)に示したような構成のレベル2のMC13を用いたチェックイン/チェックアウト、再生処理動作について説明する。

【0054】チェックアウトの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合)、SMS2に対しなされた場合について、図10を参照して説明する。

【0055】SMS2は、宿帳のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数nを調べ、 $n > 0$ のとき、デバイスID格納部4から当該LCM1のデバイスID(LCMID)を読み出し、それをMC13へ転送する(ステップS101)。

【0056】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS102)、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS103)。MC13は、さらに、識別情報格納部13bから、その識別情報(MID)を読み出して同じくLCM1へ転送する(ステップS104)。

【0057】LCM1では、MC13から転送されてきたメディアID(MID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[MID])を生成する(ステップS105)。

【0058】LCM1では、この生成された情報KM[MID]を用いて相互認証処理(AKE)を実行し、一方、MC13でも秘匿メディアID(SMID)を用

である(図8(a)参照)。

【0045】ある1つのメディアに記憶されている秘密情報が不当に読まれてしまっても、不正に使用できるのは、その秘密情報が読まれしまったメディアだけであれば問題がないわけであるから、秘密情報は、個々のメディアに固有のものであればよい。

【0046】そこで、本発明は、個々のメディアにメディア毎にそれぞれ異なる相互認証のための秘密情報を記憶させておき、この情報を用いてLCM1あるいはPD12とMC13とが相互認証を行うことにより、低コストなメディアを用いた、よりセキュリティ性の高い安全な相互認証方法を提供することを目的とする。すなわち、本実施形態で説明する相互認証方法は、図8(b)に示すように、個々のメディア(レベル2のメディア)に相互認証(AKE)のために必要な各メディア毎にそれぞれ異なる秘密情報(ここでは、秘匿メディアID(SMID)で、これは、メディアIDを何らかの方法で取得した鍵情報KMで予め暗号化されたもの)を(秘匿領域に)予め記憶させておき、LCM1、PD12には、そのメディアの識別情報(MID)を転送する。LCM1あるいはPD12側では、MIDと、先に何らかの方法で取得した情報(KM)とを用いて相互認証のための情報(メディアのもつSMIDと同じもの)を所定のアルゴリズムを用いて生成して認証処理(AKE)を行う。

【0047】このように、MC13にはそれぞれに固有の秘密情報(SMID)を持たせておくだけで、LCM1、PD12がメディアから転送されてきた各メディア毎に固有の情報(MID)を基に秘密情報(SMID)を生成することにより、メディアに負荷をかけずに安全な相互認証が行える。

【0048】なお、以下の説明において、本発明の要旨にかかる相互認証処理をAKEと呼ぶことにする。

【0049】MC13がLCM1のメディアI/F部6、あるいは、PD12にセットされると、まず、メディアI/F部6とMC13との間、あるいは、PD12とMC13との間で相互認証が行われてもよい(図9のステップS1)、そして、双方にて正当な(例えば、同じ規格のハードウェア構成である)相手であると判断されたとき(ステップS2)、メディアI/F部6あるいはPD12はMC13から読み取った識別情報MIDを基に、MC13の種別を判別する(ステップS3)。そして、メディアI/F部6あるいはPD12は、その種別に応じたチェックイン/チェックアウト/再生処理を実行する(ステップS6)。

【0050】なお、図9のステップS1における相互認証は、必ずしも図8(b)に示したような本発明の要旨にかかる相互認証である必要はない。

【0051】また、MC13にはレベル0からレベル2までの3種類があると説明したが、ここでは、レベル0

とレベル2の2種類のMC13を対象として、図9以降の複製コンテンツのチェックイン/チェックアウト/再生処理動作について説明する。

【0052】さらに、以下の説明では、省略しているが、LCM1とMC13との間、LCM1とPD12との間、PD12とMC13との間で、それぞれの秘匿領域にアクセスする際には、一方と他方との間で相互認証を行い、双方の正当性が確認されたらそれぞれの秘匿領域へのゲートを開き、秘匿領域へのアクセスが終了したら秘匿領域へのアクセスを可能にしていたゲートを閉じる仕組みになっているものとする。例えば、LCM1とMC13との間において、SMS2は、MC13の秘匿領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲードが開かれると、秘匿領域13c内に鍵情報書き込み、それが終了すると秘匿領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。

【0053】(2) レベル2のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生
図4(c)に示したような構成のレベル2のMC13を用いたチェックイン/チェックアウト、再生処理動作について説明する。

【0054】チェックアウトの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合)、SMS2に対しなされた場合について、図10を参照して説明する。

【0055】SMS2は、宿帳のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数nを調べ、 $n > 0$ のとき、デバイスID格納部4から当該LCM1のデバイスID(LCMID)を読み出し、それをMC13へ転送する(ステップS101)。

【0056】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS102)、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS103)。MC13は、さらに、識別情報格納部13bから、その識別情報(MID)を読み出して同じくLCM1へ転送する(ステップS104)。

【0057】LCM1では、MC13から転送されてきたメディアID(MID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[MID])を生成する(ステップS105)。

【0058】LCM1では、この生成された情報KM[MID]を用いて相互認証処理(AKE)を実行し、一方、MC13でも秘匿メディアID(SMID)を用

合も同様であるので、以下、PD12で再生する場合を例にとり説明する。

【0077】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし（ステップS122）、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、PD12へ転送する（ステップS123）。MC13は、さらに、識別情報格納部13bから、その識別情報（MID）を読み出して同じくPD12へ転送する（ステップS124）。

【0078】PD12では、MC13から転送されてきたメディアID（MID）をマスターキーKMで暗号化して、相互認証処理（AKE）に必要な情報（KM[MID]）を生成する（ステップS125）。

【0079】PD12では、この生成された情報KM[MID]を用いて相互認証処理（AKE）を実行し、一方、MC13でも秘匿メディアID（SMID）を用いて相互認証処理（AKE）を実行する（ステップS126）。ステップS126の相互認証処理（AKE）は、図21と同様であるので説明は省略する。

【0080】PD12とMC13との間で相互に認証されたときは、MC13では、生成した鍵情報KT（ここでは、KT2とする）を用いて秘匿領域13cに格納されていた鍵情報KT1を暗号化して（KT2[KT1]）、PD12へ転送する（ステップS127～ステップS128）。一方、PD12では、ステップS126で生成された鍵情報KT2を用いてMC13から転送されてきたKT2[KT1]を復号することができる（ステップS128）。

【0081】MC13からは暗号化されたコンテンツ復号鍵KT1[Kc]、暗号化コンテンツKc[C]を公開領域13aから読み出してPD12へ転送する（ステップS129、ステップS131）。

【0082】PD12は、鍵情報KT1の復号に成功していれば、それを用いて暗号化されたコンテンツ復号鍵KT1[Kc]を復号してコンテンツ復号鍵Kcが得られるので（ステップS130）、このコンテンツ復号鍵Kcを用いて暗号化コンテンツKc[C]を復号して、コンテンツCを得る（ステップS132）。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【0083】次に、チェックインの指示がLCM1のユーザインタフェース（I/F）部15を介して、あるいは、PD12を介して（すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合）、SMS2になされた場合について、図12を参照して説明する。

【0084】SMS2は、デバイスID格納部4から当

該LCM1のデバイスID（LCMID）を読み出し、それをMC13へ転送する（ステップS141）。

【0085】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし（ステップS142）、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、LCM1へ転送する（ステップS143）。MC13は、さらに、識別情報格納部13bから、その識別情報（MID）を読み出して同じくLCM1へ転送する（ステップS144）。

【0086】LCM1では、MC13から転送されてきたメディアID（MID）をマスターキーKMで暗号化して、相互認証処理（AKE）に必要な情報（KM[MID]）を生成する（ステップS145）。

【0087】LCM1では、この生成された情報KM[MID]を用いて相互認証処理（AKE）を実行し、一方、MC13でも秘匿メディアID（SMID）を用いて相互認証処理（AKE）を実行する（ステップS146）。

【0088】チェックインの際のステップS146の相互認証処理（AKE）動作について、図22を参照して説明する。なお、図21と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図22では、ステップS308で関数gの値が一致していたら、鍵情報KTを生成する代わりに、フラグ情報Fakeの値を「真」（図22では「T」と示している）とし、不一致のときは「偽」（図22では「F」と示している）とする（ステップS321、ステップS322）。また、LCM1では、ステップS304で関数gの値が一致していたら、鍵情報KTを生成せずに、その判断結果のみを出力する。

【0089】図12の説明に戻り、ステップS146において、LCM1がMC13を認証したときには（図22のステップS304）、MC13に対し、その秘匿領域13cに格納されている鍵情報KT1の削除を指示する。MC13では、この指示を受けると、フラグ情報Fakeの値をチェックし、「T」であれば、秘匿領域13cから鍵情報KT1を削除し、フラグ情報Fakeを「F」に書き換える（ステップS147、ステップS148）。このとき、MC13の公開領域13aに格納されている暗号化コンテンツ情報は、例えば、LCM1にて発生した乱数にて上書きすることで消去してもよい。

【0090】最後に、図7（c）に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該MC13の識別情報m0を削除する。

【0091】一方、フラグ情報Fakeの値が「F」のときは以降の処理を中止する。

【0092】次に、図10とは異なる他のチェックアウト時の処理動作について、図13を参照して説明する。なお、図10と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図13では、MC13へ転送すべきコンテンツ復号鍵Kcに対する処理に特徴がある。

【0093】図13において、LCM13では、コンテンツ復号鍵Kcに対し、まず、ステップS105で生成されたKm[MID]（以下、これをwと表す）を用いて暗号化を施す（ステップS162）。そして、wで暗号化されたコンテンツ復号鍵Kc（w[Kc]）をステップS106の相互認証処理（AKE）にて生成した鍵情報KT1を用いてさらに暗号化を行ってから（KT1[w[Kc]]）、MC13へ転送する（ステップS163）。

【0094】MC13では、ステップS106の相互認証処理（AKE）にて生成した鍵情報KT1を用いて、転送されてきたKT1[w[Kc]]を復号してw[Kc]を得、これを秘匿領域13へ格納する（ステップS164）。

【0095】コンテンツ情報Cは、図10の場合と同様に、Kcで暗号化してから（ステップS165）、MC13へ転送される（ステップS166）。

【0096】図13に示したようなチェックアウト処理動作に対応する再生処理動作について、図14を参照して説明する。なお、図11と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図14において、MC13は、秘匿領域13cに格納されている暗号化コンテンツ復号鍵w[Kc]をステップS126の相互認証処理（AKE）で生成された鍵情報KT2で暗号化してから（KT2[w[Kc]]）LCM1あるいはPD12へ転送する。（ステップS172）。LCM1あるいはPD12では、同じくステップS126で生成された鍵情報KT2でMC13から転送されてきたKT2[w[Kc]]を復号して（ステップS173）、その結果得られたw[Kc]をステップS123で生成されたw=KM[MID]を用いて復号して、コンテンツ復号鍵Kcを得る（ステップS174）。このコンテンツ復号鍵Kcを用いて暗号化コンテンツC[C]を復号して、コンテンツCを得る（ステップS175）。そして、LCM1あるいはPD12では、コンテンツCをデコーダ12hでデコードして、D/A交換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【0097】図13に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図12の説明とはほぼ同様で、異なるのは、ステップS148でMC13の秘匿領域13cから削除されるのは、鍵情報KT1ではなく、w=KM[MID]で暗号化されたコンテ

ツ復号鍵w[Kc]であるという点である。

【0098】（3）レベル0のMCを用いた複製コンテンツのチェックイン/チェックアウト/再生

次に、図4（a）に示したような構成のレベル0のMC13を用いたチェックイン/チェックアウト、再生処理動作について説明する。

【0099】この場合、MC13は、PD12にセットされ、このPD12を介してLCM1との間でチェックアウト処理が実行される。基本的な動作は、MC13がレベル2の場合と同様であるが、レベル0の場合、秘匿領域、メディアIDを有していないので、PD12がLCM1に対する処理をレベル0のMC13に代行して図10に示したような処理を実行することとなる。そのため、PD12の秘匿領域には、マスターキーKM、秘匿デバイスキーSPDID、リボケーションリスト（RVリスト）を予め記憶しておくものとする。なお、マスターキーKMは必ずしもメディアMC13に記憶しておくマスターキーKMとその機能は同じであるが、そのデータ自体は同じものである必要はない。

【0100】まず、図9のステップS3において、MC13の種別がレベル0であると判定される。

【0101】チェックアウトの指示がLCM1のユーザインタフェース（I/F）部15を介して、あるいは、PD12を介してSMS2に対しなされた場合について、図15を参照して説明する。

【0102】SMS2は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツIDが「TID1」であるとする）の子の残数nを調べ、n>0のとき、デバイスID格納部4から当該LCM1のデバイスID（LCMID）を読み出し、それをPD12へ転送する（ステップS201）。

【0103】PD12では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし（ステップS202）、登録されていないときPD12の秘匿領域にアクセスしてマスターキーKMを読み出して、LCM1へ転送する（ステップS203）。PD12は、さらに、例えばROM12cからその識別情報、すなわち、デバイスID（PDID）を読み出して、同じくLCM1へ転送する（ステップS204）。

【0104】LCM1では、PD12から転送されてきたデバイスID（PDID）をマスターキーKMで暗号化して、相互認証処理（AKE）に必要な情報（KM[PDID]）を生成する（ステップS205）。

【0105】LCM1では、この生成された情報KM[PDID]を用いて相互認証処理（AKE）を実行し、一方、PD12でも秘匿デバイスID（SPDID）を用いて相互認証処理（AKE）を実行する（ステップS206）。ステップS206の相互認証処理（AKE）は、図21と同様であるので説明は省略する。

【0106】LCM1とPD12との間で相互に認証さ

れたとき、PD12では、生成した鍵情報KT(ここでは、KT1とする)を秘匿領域に格納する(ステップS207)。LCM1では、暗号化コンテンツを復号するための復号鍵(コンテンツ復号鍵)KcをステップS206で生成された鍵情報KT1で暗号化して(KT1[Kc])、PD12を経由してMC13へ転送し(ステップS208〜ステップS209)、また、コンテンツ情報CをKcで暗号化して(Kc[C])、PD12を経由してMC13へ転送する(ステップS210〜ステップS211)。

【0107】最後に、SMS2は、図7(b)に示すように、宿帳のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数nから「1」減算し、チェックアウトリストL1に、当該MC13の識別情報「m0」を追加する。

【0108】MC13は、転送されてきた暗号化されたコンテンツ復号鍵KT1[Kc]、暗号化コンテンツKc[C]を公開領域13aに格納する。

【0109】以上の処理が終了したときのMC13の記憶内容を図6に示す。

【0110】次に、再生の指示がPD12に対しなされた場合のPD12とMC13との間の処理動作について、図16を参照して説明する。

【0111】まず、MC13は、公開領域に記録されている暗号化されたコンテンツ復号鍵KT1[Kc]をPD12へ転送する(ステップS221)。PD12が当該MC13に対し当該再生対象のコンテンツ情報をチェックアウトした際に用いたものであるならば、その秘匿領域に暗号化されたコンテンツ復号鍵を復号するための鍵情報KT1を記憶している(図15のステップS207参照)。従って、そのような正当なPD12であるならば、秘匿領域から読み出した鍵情報KT1を用いて、MC13から転送されてきたKT1[Kc]を復号して、コンテンツ復号鍵Kcを得ることができる(ステップS222)。さらに、このコンテンツ復号鍵Kcを用いて、MC13から転送されてきた暗号化コンテンツ情報Kc[C]を復号してコンテンツCを得ることができる(ステップS223〜ステップS224)。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

【0112】次に、チェックインの指示がPD12を介して(すなわち、MC13をLCM1に接続されたPD12にセットして用いて)、SMS2になされた場合について、図17を参照して説明する。この場合もチェックアウトの場合と同様、PD12がLCM1に対する処理をレベル0のMC13に代行して図12に示したような処理を実行することとなる。

【0113】SMS2は、デバイスID格納部4から当

該LCM1のデバイスID(LCMID)を読み出し、それをPD12へ転送する(ステップS231)。

【0114】PD12では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし(ステップS232)、登録されていないとき秘匿領域にアクセスしてマスターキーKMを読み出して、LCM1へ転送する(ステップS233)。PD12は、さらに、その識別情報(PDID)を読み出して同じくLCM1へ転送する(ステップS234)。

【0115】LCM1では、PD12から転送されてきたデバイスID(PDID)をマスターキーKMで暗号化して、相互認証処理(AKE)に必要な情報(KM[PDID])を生成する(ステップS235)。

【0116】LCM1では、この生成された情報KM[PDID]を用いて相互認証処理(AKE)を実行し、一方、PD12でも秘匿デバイスID(SPDI D)を用いて相互認証処理(AKE)を実行する(ステップS236)。

【0117】チェックインの際のステップS236の相互認証処理(AKE)動作は、図22において、KM[MID]をKM[PDID]に置き換え、秘匿メディアID(SMID)が秘匿デバイスID(SPDI D)に置き換えれば同様であるので、説明は省略する。

【0118】ステップS236において、LCM1がPD12を認証したときには(図22のステップS304)、PD12に対し、その秘匿領域に格納されている鍵情報KT1の削除を指示する。PD12では、この指示を受けると、フラグ情報Fakeの値をチェックし、「T」であれば、秘匿領域から鍵情報KT1を削除し、フラグ情報Fakeを「F」に書き換える(ステップS237、ステップS238)。このとき、MC13の公開領域13aに格納されている暗号化コンテンツ情報は、例えば、LCM1にて発生した乱数にて上書きすることで消去してもよい。

【0119】最後に、図7(c)に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該MC13の識別情報m0を削除する。

【0120】一方、フラグ情報Fakeの値が「F」のときは以降の処理を中止する。

【0121】次に、図15とは異なる他のチェックアウト時の処理動作について、図18を参照して説明する。なお、図15と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図18では、図13の場合と同様に、PD12へ転送すべきコンテンツ復号鍵Kcに対する処理に特徴がある。

【0122】図18において、LCM13では、コンテンツ復号鍵Kcに対し、まず、ステップS205で生成されたKm[PDID](以下、これをwと表す)を用

いて暗号化を施す(ステップS252)。そして、wで暗号化されたコンテンツ復号鍵Kc(w[Kc])をステップS251の相互認証処理(AKE)にて生成した鍵情報KT1を用いてさらに暗号化を行ってから(KT1[w[Kc]])、PD12へ転送する(ステップS253)。

【0123】PD12では、ステップS251の相互認証処理(AKE)にて生成した鍵情報KT1を用いて、転送されてきたKT1[w[Kc]]を復号してw[Kc]を得、これを秘匿領域へ格納する(ステップS254)。

【0124】コンテンツ情報Cは、図15の場合と同様に、Kcで暗号化してから(ステップS255)、PD12を経由してMC13へ転送される(ステップS256)。

【0125】図18に示したようなチェックアウト処理動作に対応する再生処理動作について、図19を参照して説明する。なお、図18と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図19において、PD12は、自身の秘匿領域に格納されている暗号化コンテンツ復号鍵w[Kc]を同じく自身の秘匿デバイスID(SPDI D=w)を用いて復号し、コンテンツ復号鍵Kcを得ることができる(ステップS261)。このコンテンツ復号鍵Kcを用いてMC13から転送されてきた暗号化コンテンツKc[C]を復号して、コンテンツCを得ることができる(ステップS262)。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D/A変換部12iでデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ(例えば音楽)を再生することができる。

【0126】図18に示したようなチェックアウト処理動作に対応するチェックイン処理動作について、図20を参照して説明する。なお、図20の説明は、図17の説明とはほぼ同様で、異なるのは、ステップS238でPD12の秘匿領域から削除されるのは、鍵情報KT1ではなく、w=KM[PDID]で暗号化されたコンテンツ復号鍵w[Kc]であるという点である。

【0127】

【発明の効果】以上説明したように、本発明によれば、低コストな記録媒体を用いて、セキュリティ性の高い安全な相互認証が実現できる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る記憶媒体(メディア)に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム(LCM)の構成例を示した図。

【図2】メモリ領域の構成例を示した図。

【図3】記録再生装置(PD)の内部構成例を示した図。

【図4】3種類の記憶媒体の特徴を説明するための図。

【図5】メディアインタフェース(I/F)部の内部構成例を示した図。

【図6】チェックイン後の記憶媒体の記録内容を説明するための図。

【図7】LCMの秘匿領域に格納されている宿帳の記憶例を示した図。

【図8】相互認証方法の概略を説明するための図。

【図9】チェックイン/チェックアウト処理手順を説明するためのフローチャートで、メディアの種別を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図10】記録媒体の種別がレベル2の場合のチェックアウト時の手順を説明するための図。

【図11】記録媒体の種別がレベル2の場合の再生時の手順を説明するための図。

【図12】記録媒体の種別がレベル2の場合のチェックイン時の手順を説明するための図。

【図13】記録媒体の種別がレベル2の場合のチェックアウト時の他の手順を説明するための図。

【図14】記録媒体の種別がレベル2の場合の再生時の他の手順を説明するための図。

【図15】記録媒体の種別がレベル0の場合のチェックアウト時の手順を説明するための図。

【図16】記録媒体の種別がレベル0の場合の再生時の手順を説明するための図。

【図17】記録媒体の種別がレベル0の場合のチェックイン時の手順を説明するための図。

【図18】記録媒体の種別がレベル0の場合のチェックアウト時の他の手順を説明するための図。

【図19】記録媒体の種別がレベル0の場合の再生時の他の手順を説明するための図。

【図20】記録媒体の種別がレベル2の場合のチェックイン時の他の手順を説明するための図。

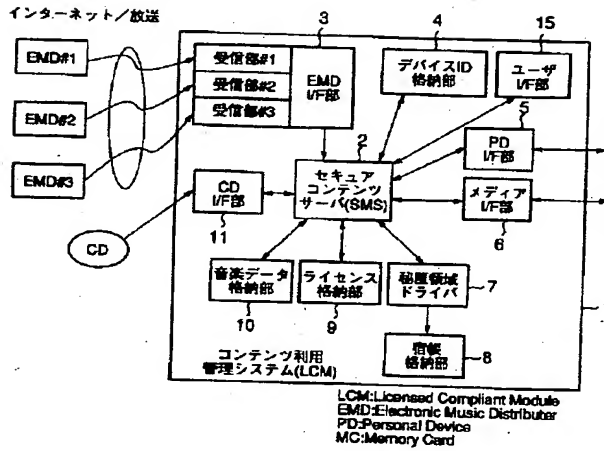
【図21】相互認証処理(AKE)の処理動作について説明するための図。

【図22】相互認証処理(AKE)の他の処理動作について説明するための図。

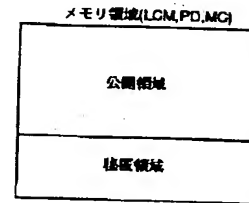
【符号の説明】

- 1…LCM(コンテンツ利用管理システム)
- 2…SMS(セキュア・コンテンツ・サーバ)
- 3…EMDインタフェース部
- 4…デバイスID格納部
- 5…PDインタフェース部
- 6…メディアインタフェース部
- 7…秘匿領域ドライバ
- 8…宿帳格納部
- 9…ライセンス格納部
- 10…音楽データ格納部
- 50 11…CDインタフェース部

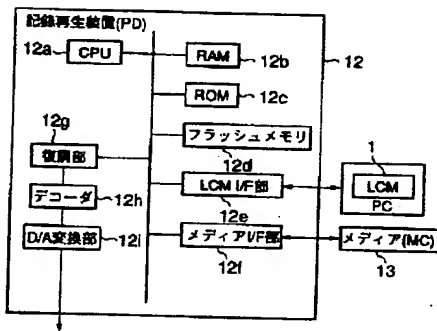
【図1】



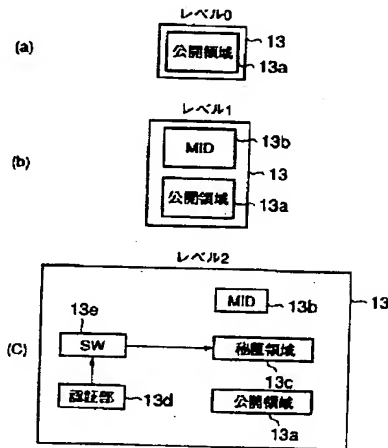
【図2】



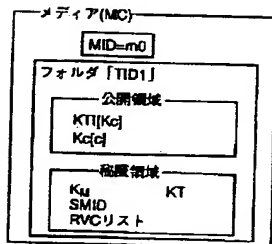
【図3】



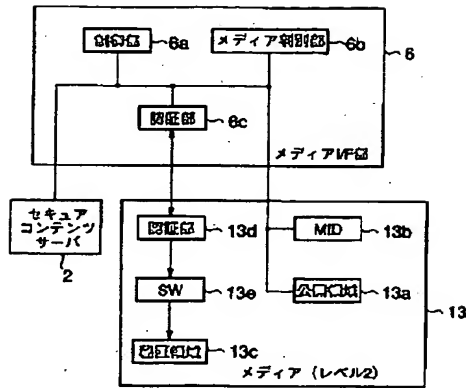
【図4】



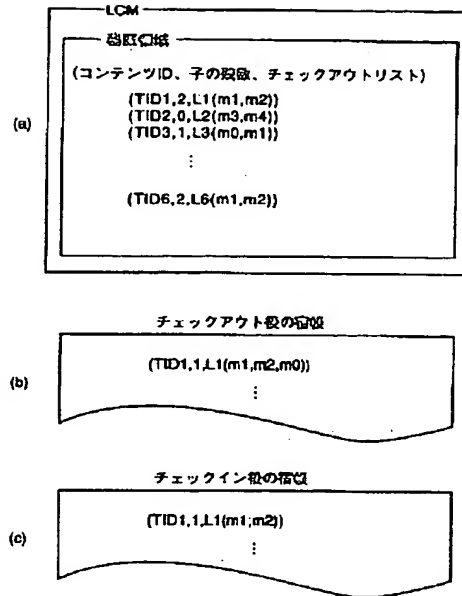
【図6】



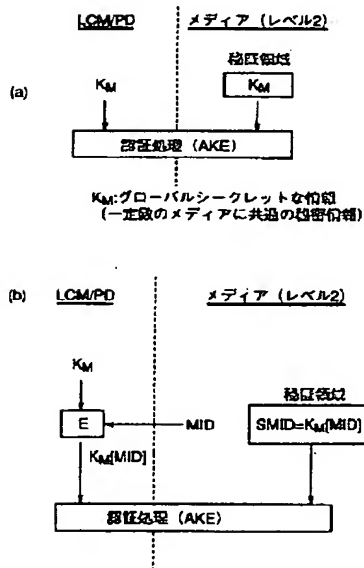
【図5】



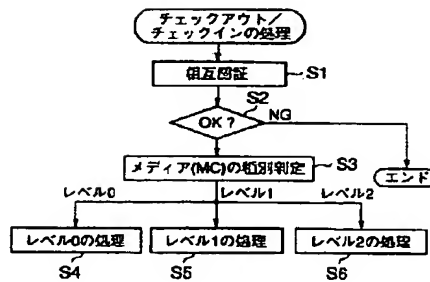
【図7】



【図8】

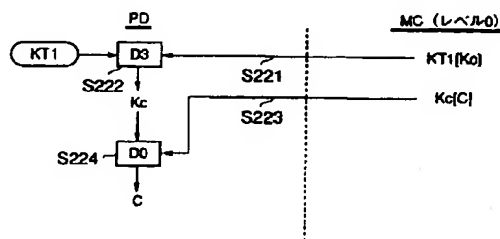


【図9】

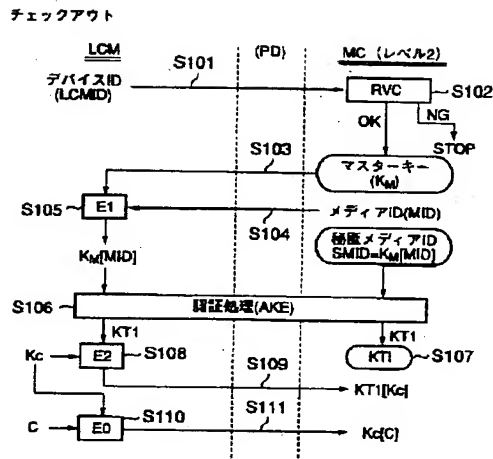


【図16】

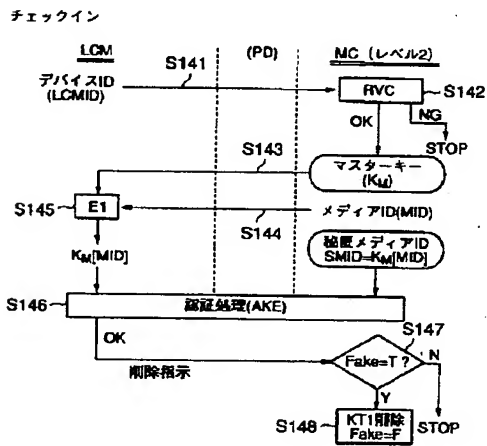
再生



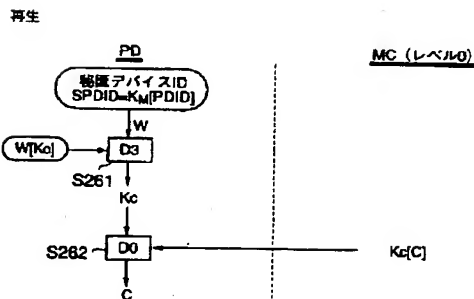
【図10】



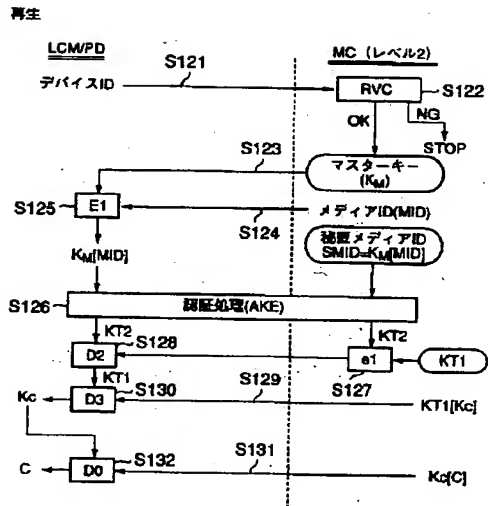
【図12】



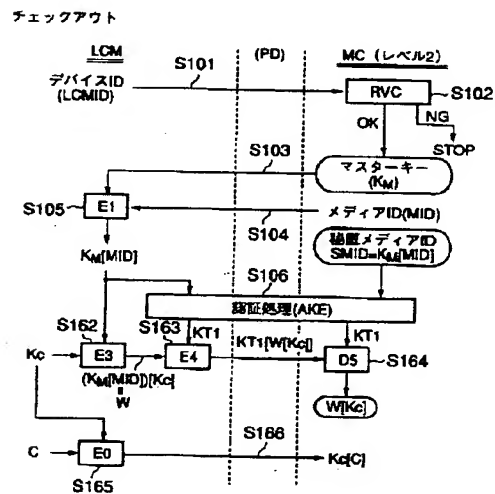
【図19】



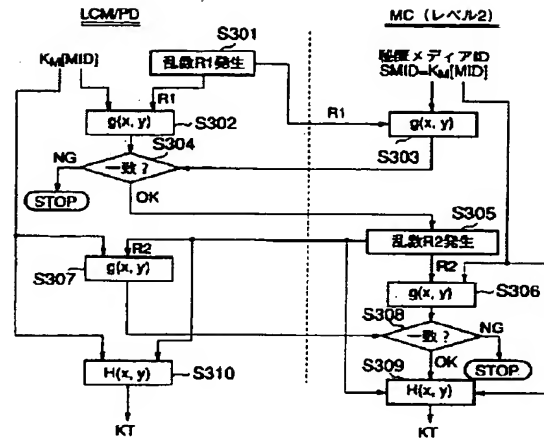
【図11】



【図13】



【図21】



The diagram illustrates the authentication sequence across three components: LCM, PD, and MC (レベル0). The process is divided into two main phases by a vertical dashed line.

LCM (Left):

- S201:** LCM sends **デバイスID (LCMID)** to PD.
- S203:** LCM sends **マスターキー (K_M)** to E1.
- S204:** LCM sends **デバイスID (PDID)** to E1.
- S205:** E1 outputs **K_M [PDID]** to the **認証処理 (AKE)** block.
- S206:** The **認証処理 (AKE)** block outputs **KT1** to E2.
- S208:** E2 outputs **K_C** to E0.
- S210:** E0 outputs **C** to the MC.

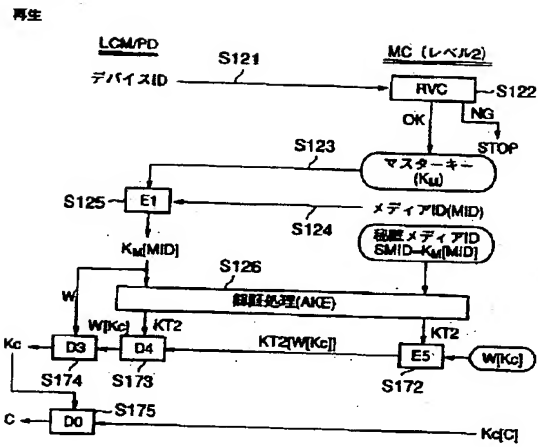
PD (Middle):

- S202:** PD receives **デバイスID (LCMID)** and outputs **S202** to MC.
- OK/NG:** PD outputs **OK** or **NG** to the **マスターキー (K_M)** block.
- STOP:** PD outputs **STOP** to the **マスターキー (K_M)** block.
- S207:** PD outputs **KT1** to MC.

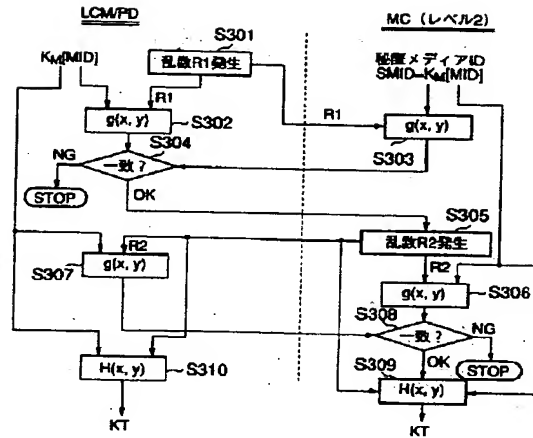
MC (レベル0) (Right):

- S202:** MC receives **S202** from PD.
- S209:** MC receives **KT1 [K_C]** from E2.
- S211:** MC receives **K_C [C]** from E0.

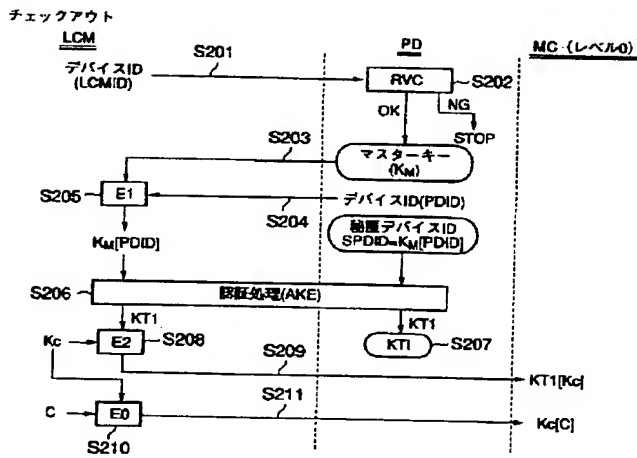
【図14】



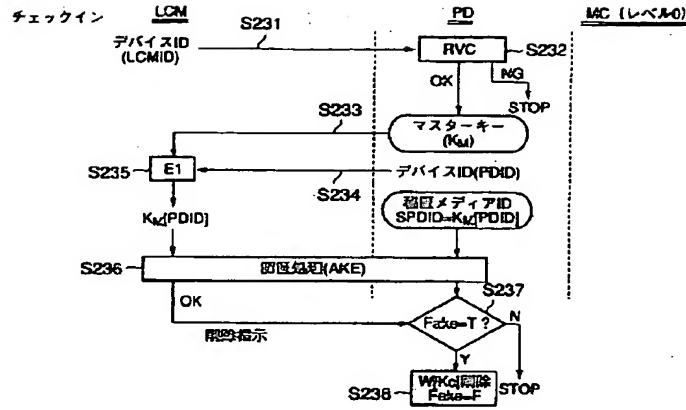
【図21】



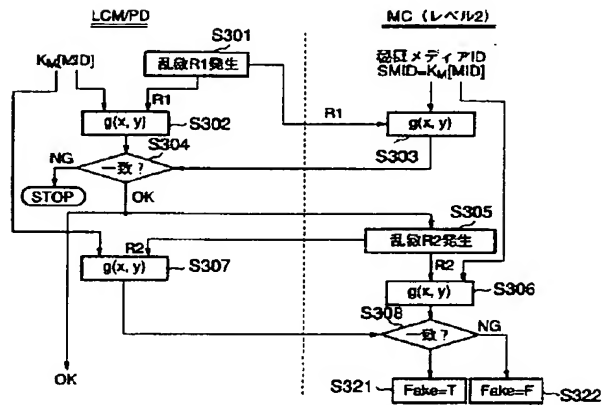
【図15】



【図20】



【図22】



フロントページの続き

(72)発明者 山田 尚志
東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内

(72)発明者 岩崎 博
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝マイクロエレクトロニクスセン
ター内

(72)発明者 田村 正文
東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内

(72)発明者 石橋 泰博
東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72)発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中工場内

(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 原田 俊治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(18)

特開2000-357213

F ターム(参考) 5B058 KA31 YA16
5B065 BA02 BA03 BA09 PA02 PA04
PA11
5B085 AE06 AE12 AE23